SYLOW THEOREMS

Recall: (FIRST SYLOW THEOREM) Let G be a finite group, $|G| = p^e N$ $p \nmid N$.

Then p-sylow subgroup of G exists.

SECOND SYLOW THM:

$$|G| = p^e N \quad p \nmid N$$

1) p-Sylow subgroups of G are conjugates

2) Every p-subgroup of G is contained in some p-Sylow subgroup of G.

THIRD SYLOW THM:

If s is the number of p-Sylow subgroups of G, then

$$s \mid N \quad \text{and} \quad s \equiv 1 \pmod{p}.$$

→ Every group of order 15 is cyclic.

$$|G| = 3 \cdot 5$$

No. of 3- Sylow subgroups $| 5$

and $\equiv 1 \pmod 3$

$\Rightarrow$ There is exactly one 3-Sylow subgroup, say H.

No. of 5- Sylow subgroups $| 3$

and $\equiv 1 \pmod 5$

$\Rightarrow$ There is exactly one 5- Sylow subgroup, say K.

Both are normal in G, because gHg^{-1} is a subgroup of size 3, hence $gHg^{-1} = H$.

Similarly $gKg^{-1} = K$.

So, $HK \cong H \times K \cong G \Rightarrow G \cong \mathbb{Z}/3 \times \mathbb{Z}/5$
$= \mathbb{Z}/15\mathbb{Z}$

Problem: Classify all groups of order $99 = 3^2 \times 11$ up to isomorphism.

INTRODUCTION TO RINGS

Defn: A ring R is a set with two binary operations, addition and multiplication such that

1) $(R, +)$ is an abelian group
2) Multiplication is associative, has an identity 1.
3) Distributive property holds

$$a(b+c) = ab + ac \qquad \forall\ a, b, c \in R$$
$$(a+b)c = ac + bc$$

If multiplication is commutative, R is called a commutative ring, otherwise R is called non-commutative ring.

Examples: 1) $\mathbb{Z}$ - Commutative

2) $\mathbb{R}$, $\mathbb{C}$ - Commutative

3) $M_{n\times n}(R) = \left\{ \begin{array}{l} \text{Set of all } n\times n \text{ matrices} \\ \text{with entries in } R \end{array} \right\}$

└ non-Commutative

4) $\mathbb{Z}/n\mathbb{Z}$ - Commutative

5) $\{0\}$ - Commutative

Lemma: $R = \{0\} \iff 1 = 0$

Pf: $\Rightarrow$ Clear

$\Leftarrow$ Assume $1 = 0$.

Then $a = a \cdot 1 = a \cdot 0 = 0$.

So, $R = \{0\}$.

6) Polynomial Rings

R commutative ring

$$R[x] = \left\{ a_0 + a_1 x + \cdots + a_n x^n \;\middle|\; \begin{matrix} n \in \mathbb{N} \\ a_i \in R \end{matrix} \right\}$$

$$\begin{aligned} & a_0 + a_1 x + \cdots + a_n x^n \\ + \; & b_0 + b_1 x + \cdots + b_n x^n \end{aligned} = \begin{aligned} & (a_0 + b_0) + (a_1 + b_1) x \\ & + \cdots + (a_n + b_n) x^n \end{aligned}$$

$$(a_0 + a_1 x + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m)$$

$$= a_0 (b_0 + b_1 x + \cdots + b_m x^m) + \cdots$$

Characteristic of a Ring

Defn: We say that n is the characteristic of a ring R, (also denoted as char R) if n is the smallest positive integer such that $\underbrace{1+1+\cdots+1}_{n \text{ times}} = 0$.

If no such n exists, we say $\text{char}(R) = 0$.

Examples:

1) $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$ char 0 rings

2) $\mathbb{Z}/n\mathbb{Z}$ char n

Subrings and Ideals

Defn: A *subring* S of R is a subgroup of R under $+$, closed under multiplication and contains 1.

Qn: What are all subrings of $\mathbb{Z}$?

Defn: An *ideal* I of a ring R is a subset of R that satisfies:

i) $(I, +)$ is a subgroup of R.

ii) For any $r \in R$, $s \in I$
$rs \in I$.

Examples: 1) $I = \{0\}$ is an ideal of every ring R.

2) $I = R$ is an ideal of R.

3) What are all ideals of $\mathbb{Z}$?

Polynomial Ring $\mathbb{Z}[x]$

We can divide in $\mathbb{Z}[x]$!

Given two polynomials $f(x), g(x)$ $(\deg f \leq \deg g)$ there exists a quotient $(q(x))$ and remainder $(r(x))$ such that

$$g(x) = f(x)\, q(x) + r(x) \qquad \deg r < \deg f \text{ or } r = 0$$

$\mathbb{Z}$	$\mathbb{Z}[x]$
Absolute value	degree
Division algorithm	Division algorithm

Ideals in $\mathbb{Z}[x]$

Example:

$$I = \{ x f(x) \mid f(x) \in \mathbb{Z}[x] \}$$

$$= \langle x \rangle$$

In general every ideal I of $\mathbb{Z}[x]$ is of the form

$$I = \langle f(x) \rangle \quad \text{for some } f \in \mathbb{Z}[x].$$

Proof: Choose $f(x)$ as a polynomial with smallest degree in I.

If $g(x) \in I$, then

$$\underbrace{g(x)}_{\in I} = \underbrace{f(x)\, q(x)}_{\in I} + r(x)$$

$\Rightarrow$ $r(x) \in I$ but $\deg r < \deg f$ is not possible

$\Rightarrow$ $r(x) = 0$

So, $I = \langle f(x) \rangle$

$\downarrow$

Ideals of this form are called <u>principal ideals</u>.

In $\mathbb{Z}$ and $\mathbb{Z}[x]$, every ideal is principal.